

# Lieutenant Governor André Bauer's



## Senior Fraud Prevention Resource Guide

Office of the Lieutenant Governor  
Office on Aging  
1301 Gervais Street Suite 200  
Columbia, SC 29201  
Phone: (803) 734-9900  
[www.aging.sc.gov](http://www.aging.sc.gov)

For updates from the Office on Aging visit [www.aging.sc.gov](http://www.aging.sc.gov) and  
click the email update link.

---

## **Table of Contents**

---

<b>I. Introduction.....</b>	<b>3</b>
<b>II. Scams .....</b>	<b>5</b>
<b>III. Identity Theft.....</b>	<b>11</b>
<b>IV. Banking and Financial Institutions.....</b>	<b>16</b>
<b>V. Medicare.....</b>	<b>21</b>
<b>VI. How to Help Yourself.....</b>	<b>26</b>
<b>VII. Filing a Complaint with the South Carolina Department of Consumer Affairs.....</b>	<b>27</b>
<b>VIII. Filing a Complaint with the Lt. Governor's Office on Aging.....</b>	<b>28</b>
<b>IX. Fraud Complaint Form.....</b>	<b>29</b>
<b>X. Resources.....</b>	<b>31</b>

---

## INTRODUCTION

---

Every year, hundreds of South Carolina seniors fall victim to some kind of financial exploitation. With the number of citizens 60 years and older expected to double over the next two decades, the count is expected to increase dramatically. To combat this endangerment to seniors, Lieutenant Governor Andre Bauer has created this important resource with practical steps to safeguard our citizens from being victimized by fraud.

In April 2008, the South Carolina General Assembly adopted Resolution H.5025, which stated that when seniors are scammed of their life savings and independence, “it falls to government to provide support to those senior adults who have been financially exploited through calculating theft of their resources by unscrupulous persons.” Legislators urged “coordination of government and private resources in the State of South Carolina to protect our senior citizens from scams and other schemes that undermine their financial independence.” They tasked the Lieutenant Governor's Office on Aging to coordinate with the Department of Consumer Affairs, Office of Secretary of State, Office of Attorney General, South Carolina Educational Television, South Carolina Law Enforcement Division, Adult Protection Coordinating Council, and other state agencies, private groups, local law enforcement, solicitors, magistrates, and media organizations to shield our senior citizens from fraudulent businesses and individuals who seek to take what South Carolina seniors have worked so hard to obtain their entire lives.

### **What is Exploitation?**

South Carolina's Omnibus Adult Protection Act defines exploitation as:

- (a) causing or requiring a vulnerable adult to engage in activity or labor which is improper, unlawful, or against the reasonable and rational wishes of the vulnerable adult. Exploitation does not include requiring a vulnerable adult to participate in an activity or labor which is a part of a written plan of care or which is prescribed or authorized by a licensed physician attending the patient;
- (b) an improper, unlawful, or unauthorized use of the funds, assets, property, power of attorney, guardianship, or conservatorship of a vulnerable adult by a person for the profit or advantage of that person or another person; or
- (c) causing a vulnerable adult to purchase goods or services for the profit or advantage of the seller or another person through: undue influence, harassment, duress, force, coercion, or swindling by overreaching, cheating, or defrauding the vulnerable adult through cunning arts or devices that delude the vulnerable adult and cause him/her to lose money or other property.

## **Why would someone want to take advantage of me?**

There are many reasons why people deceive seniors. The most common are:

**Entitlement:** A person may feel they are entitled to your money based on lineage or they may feel that you do not require all the money you have.

**Opportunity:** A person may take advantage of another's trust and goodwill by pressure and influence.

**Necessity and Greed:** A person, who is experiencing financial difficulties and is consumed by greed, may take advantage of a person's kindness.

## **Why do these types of crime go unreported?**

- Embarrassment
- Blaming oneself for being taken advantage of
- Relationship with offender
- Fear of consequence(s) if family members find out
- Not understanding that these acts are crimes
- Intimidated by the criminal justice system
- Fear that the crime cannot be proven
- Lack of understanding about the reporting process
- Fear of retaliation

## **Scams**

---

There are several types of scams floating around geared toward stealing your hard earned money. In this section we will detail each scam and provide ways to protect you from being taken advantage of.

### ***Deceptive Sales Practices***

Beware of merchants or salespersons that use high-pressure tactics or unusual ploys. Following are examples of such tactics or gimmicks that are used:

#### ***Bait and switch:***

A store may advertise a special low price. When the consumer asks about that item, the salesperson will try to switch the consumer's attention to a more expensive article.

#### ***High pressure tactics:***

A salesman will forcefully try to pressure you into buying something. The salesman is trained to make the deal sound irresistible, and you might well buy something without thinking the matter through. In such a situation, you should insist on a delay. Take time to get the opinion of a friend or relative in order to gain time to "cool off" and consider the purchase more carefully. If the salesman is legitimate and believes in his or her product, the salesman will not object to a delay. If the salesman persists strongly, back off.

#### ***Referral sales:***

These schemes operate by promising you a fee to be paid for each new customer referred to them as a potential client. In theory, if you send the store enough business, the item you want to buy is practically free. In reality the process is much like a chain letter. All prospective customers meeting the seller's requirements are quickly used, leaving most customers to pay the full price. In addition, goods are usually marked up, so you gain little or nothing from any discounts you receive. This kind of scheme is now illegal in South Carolina. But if you should get drawn in by similar schemes, see an attorney or report this matter to the Department of Consumer Affairs.

#### ***Door to Door Sales:***

*Keep in Mind that Medicare and Social Security do not make home visits. See page for more information on Medicare rules.*

The first thing you should remember about door to door salesmen is that you do not have to talk to them. If you do not want to buy anything, all you have to do is ask the salesman to leave.

A South Carolina law allows you three days to cancel a home solicitation sale, and a Federal Trade Commission (FTC) rule allows you three days to cancel a cash purchase of \$25.00 or more.

If you do decide to cancel the sale or rescind the contract, you must do so by sending written notice to the company or business before midnight of the third business day following the date of the transaction. Keep a copy for your records.

South Carolina law requires a notice to cancel is given to the customer and to have a conspicuous caption that clearly states, "BUYER'S RIGHT TO CANCEL." The notice must also include the following: 'If you decide you do not want the goods or services, you may cancel this agreement by mailing a notice to the seller.' The notice must say that you do not want the goods or services and must be mailed before midnight of the third business day after you sign this agreement. The notice must be mailed to: (name and mailing address of seller). The Federal Trade Commission also requires a Notice of Cancellation to be given to you, along with copies of the receipt or sales contract.

Once the merchant receives the notice or letter of cancellation, he has 10 days to refund any money that he has received, return any documents that you may have signed, return any goods or property that you have traded in and inform you that he will pick up or let you keep any items that were left with you. Products left with you must be available to the seller in the same condition as you received them. It is not your responsibility to ship the items back to the seller or pay postage expenses for such shipping. The seller must pay the return postage expenses.

### ***Pest control fraud:***

This type of fraud is prevalent in the South where there are large problems with insects. This can usually take the form of a termite inspector who appears and informs you that termites have infested your home, but if you contract for his or her services today, you will receive a discount. Always avoid such pressures. It is extremely doubtful that your house will start tumbling down that very day. Besides not applying pesticides properly, the fraudulent pest control worker may not use a recognized or effective pesticide. As a matter of fact, he or she may apply a liquid that just smells like a chemical but does not have any effect at all.

Don't deal with door-to-door pest control operators. If you need their services, check the Yellow Pages, then call them and ask for an estimate based on your needs.

- Always ask to see a salesman's license to solicit and verify their company and identity, before letting them into your home.
- Make sure you personally read and understand anything you are asked to sign. Keep records of the salesman's name, company, address, telephone number, and date of transaction.

***Telemarketing:***

Live telephone solicitors must identify themselves, their business and the object of the call and, within 30 seconds after beginning the conversation, state the purpose of the call and allow you the opportunity to respond. If you say you are not interested, the solicitor must discontinue the call and remove your name and telephone number from the list if you ask not to be called again. Live telephone solicitation calls may not be made after 9:00 p.m. or before 8:00 a.m. and must disclose the cost of merchandise or method of estimation, payment plan, and extra or special charges like shipping, handling and taxes. You should contact the Department of Consumer Affairs if you have any complaints about the violation of this law. The department can impose a monetary penalty against the telephone solicitor if necessary. Violation of this law can also be prosecuted as a crime.

***Telephone Schemes:***

Have you ever received a telephone call with the person on the other end saying “Act Immediately!” “This is a once in a lifetime opportunity!” or “You’ve won a prize!”? Do not fall for this type of scheme. The person on the other end wants to steal your money. These con artists are trying to obtain valuable personal information such as your Social Security number, checking account number, credit card numbers and even driver’s license number. With just that little bit of information, they can rob you blind.

- Never give out personal information over the phone unless you’ve initiated the call.
- Never allow anyone to pressure you into acting immediately over the phone.
- Never agree to or accept an offer until you’ve seen it in writing.
- Never pay for a “prize” over the telephone.

**National Do Not Call Registry**

There is something you can do about unwanted telephone calls made to you for purposes of selling you something. The FCC has established a national Do Not Call Registry. Once your residential or cellular telephone number has been listed on the registry for 30 days, telemarketers are prohibited from calling that number. You can report any violations directly to the FCC. To register for the national Do Not Call Registry go to [www.donotcall.gov](http://www.donotcall.gov) or call 1-888-382-1222.

### ***Mail Fraud:***

Mail has just arrived and you've received an official looking letter with a shiny seal with the words "Official Document" or "Official Government Business" stamped or printed across it. You open the letter and find that it's a company claiming you've won a prize. Others may claim to be non-profit organizations looking for donations to support diabetes, breast cancer, etc. BEWARE! A growing number of these organizations are not legitimate.

- Never give money or credit card numbers out to enter sweepstakes or contests.
- Do not respond to letters asking you to call them for information on how to claim your prize.
- Always research organizations you donate money to in order to make sure they are legitimate.

### ***Phishing:***

According to the National Consumers League, the most common form of phishing is by email. Pretending to be from a legitimate retailer, bank, or government agency, the sender asks to "confirm" your personal information for some made-up reason. Typically, the email contains a link to a phony web site that looks just like the real thing. You enter your personal information on the web site — and send it into the hands of identity thieves.

Phishers also use the phone to hunt for victims' personal information. Some pose as employers and call or send emails to people who have listed themselves on job search Web sites. Don't click on links in emails that ask you to provide personal information. To check whether an email or call is really from the company or agency, contact it directly by phone or by going online. If you don't have the telephone number, get it from the phone book, directory assistance, or the Internet. Use a search engine to find the official Web site.

- Never provide account information or passwords in response to an email request.
- Do not buy into their scare tactics that claim that failure to respond to them will create consequences.
- Always report suspicious e-mails. You can do this by contacting the National Consumers League's National Fraud Information Center at [www.fraud.org](http://www.fraud.org) or toll-free 1-800-876-7060.



## **Other Common Scams**

---

### ***Phone company scam:***

While pretending to be a representative from a local phone company, the perpetrator purports that a problem exists on the telephone line. The perpetrator asks the victim to call back under the guise of conducting a test. This allows the perpetrator to make long distance phone calls and bill them to the victim.

### ***Charitable donation scam:***

Scam artists claiming to represent charitable organizations use e-mails and telephone calls to steal donations and in some cases donors' identities.

### ***Advance fee fraud or “419” fraud:***

Named after the relevant section of the Nigerian Criminal Code, this fraud is a popular crime with West African organized criminal networks. There are a myriad of schemes and scams—mail, email, fax and telephone promises are designed to facilitate victims' giving money presumably to bribe government officials involved in the illegal conveyance of millions outside the country. Victims are to receive a percentage for their assistance.

### ***Pigeon drop:***

The victim puts up "good faith" money in the false hope of sharing the proceeds of an apparent large sum of cash or item(s) of worth which are "found" in the presence of the victim.

### ***Financial institution examiner fraud:***

The victim believes that he or she is assisting authorities to gain evidence leading to the apprehension of a financial institution employee or examiner that is committing a crime. The victim is asked to provide cash to bait the crooked employee. The cash is then seized as evidence by the “authorities” to be returned to the victim after the case.

### ***Inheritance scams:***

Victims will receive mail from an "estate locator" or “research specialist” claiming that an unclaimed inheritance or refund has been located and belongs to you. The victim is lured into sending a fee to receive information about how to obtain the purported asset.

***Financial institution employee fraud:***

The perpetrator calls the victim pretending to be a security officer from the victim's financial institution. The perpetrator advises the victim that there is a system problem or internal investigation being conducted. The victim is asked to provide his or her Social Security number for "verification purposes" before the conversation continues. The number is then used for identity theft or other illegal activity.

***Misappropriation of income or assets:***

A perpetrator, often a family member or caregiver, obtains access to a vulnerable adult's security checks, pension payments, checking or savings account, credit card or ATM, or withholds portions of checks cashed for an elder adult.

***Fictitious relative:***

The perpetrator calls the victim pretending to be a relative in distress and in need of cash and asks that money be transferred either into a financial institution account or wired.

***Government grant scams:***

Victims are called with the claim that the government has chosen their family to receive a grant. In order to receive the money, victims must provide their checking account number and/or other personal information. The perpetrator may electronically debit the victim's account for a processing fee, but the grant money is never received.

***Spoofing:***

An unauthorized website mimics a legitimate website for the purpose of deceiving consumers. Consumers are lured to the site and asked to log in thereby providing the perpetrator with authentication information that the perpetrator can use at the victim's legitimate financial institution's website to perform unauthorized transactions.

***Pharming:***

A malicious Web redirect sends users to a criminal's spoofed site even though the user entered a valid URL in the browser's address bar. This redirection usually involves worms and Trojans or other technologies that attack the browser address bar and exploit vulnerabilities in the operating systems and Domain Name Servers (DNS) of the compromised computers.

***Stop Foreclosure Scam:***

The perpetrator claims to be able to instantly stop foreclosure proceedings on the victim's real property. The scam often involves the victim deeding the property to the perpetrator who says that the victim will be allowed to rent the property until some predetermined future date when the victim's credit will have been repaired and the property will be deeded back to the victim without cost. Alternatively, the perpetrator may offer the victim a loan to bridge his or her delinquent payments, perhaps even with cash back. Once the paperwork is reviewed, the victim finds that his or her property was deeded to the perpetrator. A new loan may have been taken out with an inflated property value with cash back to the perpetrator, who is now the property owner. The property very quickly falls back into foreclosure and the victim, now tenant, is evicted.

***Investment Property:***

Property is sold to the vulnerable adult as a guaranteed investment with high yield returns. The victim is convinced to buy investment property through, or in conjunction with, a property management firm that will handle all the loan documents, make all the loan payments, place the tenants, collect the rents and maintain the property. The victim is told that he or she has to do nothing other than be the buyer and borrower. The property then falls into foreclosure. The victim finds that the property was inflated in value, payments at the closing were made to the property management company or affiliated parties, no loan payments have ever been made, and any collected rents have been stolen as well.

***International lottery fraud:***

Scam operators, often based in Canada, use telephone and direct mail to notify victims that they have won a lottery. To show good faith, the perpetrator may send the victim a check. The victim is instructed to deposit the check and immediately send (via wire) the money back to the lottery committee. The perpetrator will create a "sense of urgency," compelling the victim to send the money before the check, which is counterfeit, is returned. The victim is typically instructed to pay taxes, attorney's fees and exchange rate differences in order to receive the rest of the prize. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

***Identity Theft***

---

According to the Federal Trade Commission, identity theft occurs when someone uses your personal identifying information, such as your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes. For identity thieves, this information is as good as gold.

Skilled identity thieves may use a variety of methods to collect all of your information, including:

***Dumpster Diving:*** They rummage through trash looking for bills or other paper with your personal information on it.

***Skimming:*** They steal credit/debit card numbers by using a special storage device when processing your card.

***Phishing:*** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.

***Changing Your Address:*** They divert your billing statements to another location by completing a change of address form.

***Old-Fashioned Stealing:*** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.

***Pre-texting:*** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

**Once they have your personal information, identity thieves use it in a variety of ways.**

***Credit card fraud:***

- They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.
- They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

***Phone or utilities fraud:***

- They may open a new phone or wireless account in your name, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

***Bank/finance fraud:***

- They may create counterfeit checks using your name or account number.
- They may open a bank account in your name and write bad checks.
- They may clone your ATM or debit card and make electronic withdrawals using your name, thus draining your accounts.
- They may take out a loan in your name.

***Government documents fraud:***

- They may get a driver's license or official ID card issued in your name but with their picture.
- They may use your name and Social Security number to get government benefits.
- They may file a fraudulent tax return using your information.

***Other fraud:***

- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

***Phony Employment Fraud:***

- You are being paid to conduct wire transfers through your account
- You respond to a company making fraudulent employment offers such as work-from-home, envelope stuffing, secret shoppers, and home accounting positions.

***Important Questions to Ask Yourself:***

- Is the check from an item you sold on the internet? Such as a car, boat, jewelry, etc.
- Is the amount of the check more than the item's selling price?
- Did you receive the check through an overnight delivery service?
- Is the check drawn on a business or individual different from the person buying your item or product?
- Have you been informed that you were the winner of a lottery, such as a Canadian, Australian, El Gordo, or El Mundo lottery, that you did not enter?
- Have you been instructed to either "WIRE", "SEND", or "SHIP" money, as soon as possible to a large US city or to another country such as Canada, England, or Nigeria?
- Have you been asked to pay money to receive a deposit from another country such as Canada, England, or Nigeria?
- Did you respond to an e-mail requesting you "RESPOND", "CONFIRM" OR "PROVIDE" your account information?

If you answered yes to any of these questions provided by the Federal Bureau of Investigation, please contact the LGOA by emailing [scams@aging.sc.gov](mailto:scams@aging.sc.gov) or calling 1-800-868-9095 or the Department of Consumer Affairs at 800-922-1594.

### **How to Safeguard Your Identity:**

- Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Ask if you can use a password instead.
- Never have your Social Security number printed on you checks
- Secure personal information in your home, especially if you have roommates, employ outside help, or are having work done in your home.
- Ask about information security procedures in your workplace or at businesses, doctor's offices, or other institutions that collect your personally identifying information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well.
- Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.
- Order a copy of your credit report from each of the three major credit reporting agencies (Equifax, TransUnion, and Experian) every year to make sure it is accurate. You can receive a free copy of your credit report once a year by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-322-8228.

## **Financial Identity Fraud and Identity Theft Protection Act**

South Carolina consumers can do more to protect their identity now that the General Assembly passed and Governor Mark Sanford signed the “Financial Identity Fraud and Identity Theft Protection Act” on April 2, 2008. The Act provides much needed protection for consumers and is one of the most consumer-friendly and comprehensive bills of its kind in the nation. A primary provision in the bill allows consumers to freeze and thaw their credit report at no charge. Any consumer may place a freeze on their report, including those wanting to take proactive measures to protect themselves against identity thieves or not wanting to receive more credit than they can financially handle. Businesses, however, have no need to worry about consumers not being able to make purchases as they choose. Thawing your credit only takes one phone call and 15 minutes. South Carolina is one of only two states in the country that provides this service to consumers free of charge. The Act also provides requirements in the area of credit report disputes that are similar to those in the Federal Fair Credit Reporting Act. Under the Financial Identity Fraud and Identity Theft Protection Act, credit reporting agencies must follow certain procedures when a consumer notifies it of an inaccurate or untimely item on their credit report. The consumer is also given the right to sue a credit reporting agency if it does not comply with the Act. This portion of the act will be effective December 31, 2008.

In addition to giving consumers more control with their credit, the bill also addresses identity theft concerns. According to the Act, organizations and businesses who maintain consumers’ personal information must now alert consumers when their personal information may have been compromised. Notice of the security breach must also be given to the Department if 1000 more South Carolina consumers were affected. The Department has been given the responsibility of ensuring consumer are being informed when their identity has been compromised internally or externally. This portion of the bill will be effective July 1, 2009.

The bill also requires all organizations and businesses collecting personal information to have measures for the safe disposal of material “in a manner that makes it unreadable or undecipherable.” The Department has been tasked to ensure this requirement is satisfied. This portion of the bill will also be effective July 1, 2009.

Other provisions of the Act include making identity theft a crime, prohibiting dumpster diving, putting restrictions on the use of social security numbers, and limiting the information on credit card receipts.

### ***Home Improvement Fraud:***

Con artists are always looking for ways to prey on trusting homeowners. Because of this, the S.C. Department of Labor and the Licensing and Regulation's Residential Builders Commission has provided some tips to help further educate homeowners about home improvement fraud. The LLR states that the biggest problem is that homeowners are paying way too much money up front for improvements. Many of these unlicensed contractors may quote you a low price, and once paid, take off with your money. Keep in mind that honest contractors never ask for a large sum of money up front.

- Get at least two bids and do not automatically choose the lowest.
- Ask for local references and contact them.
- Contact the Residential Builder's Commission at 1-803- 896-4696 to see if the contractor is licensed or if he or she has any complaints against them.
- Make sure the contractor is bondable.
- Never pay for an entire job up front. The down payment should be no more than 1/3 the contract price.
- Be specific about what you want done. Put all details in writing if possible.
- Check with appropriate local building officials concerning permits.

## **Banking and Financial Institutions**

### ***Opening a New Account:***

When opening a new account, always make sure to bring two forms of identification. You will be asked your name, address, date of birth, and Social Security number. To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record this information.

Once given an account kit, always make sure to read the privacy policy, schedule of fees, depositor's agreement, and truth in savings brochures. These brochures detail everything from fees associated with your account, how interest is calculated, the selling of third party information, etc.



***Privacy Policy and Opting Out:***

In banking, a privacy policy must be given every time a person opens a new account. Always read this document. It details how your individual bank safeguards or discloses your personal information. Most banks will share your information with their affiliated third parties, unless you opt out from being contacted. If you prefer that your customer information not be shared, always fill out your opt out disclosure which is attached to the privacy policy. We recommend you seriously consider “opting out.”

***Setting up direct deposit:***

Setting up direct deposit for any type of income that comes in is always in a person’s best interest. This is one of the best ways to help safeguard yourself from having your paychecks, retirement checks, or personal checks, from being stolen in the mail. Using direct deposit will assure that your money will be in your account on a set day every month. To have your Social Security or Social Security income check directly deposited into your account, you can log on to <http://www.security.gov/deposit> or contact Social Security at 1-800-772-1213.

***Online banking and bill pay:***

Using online banking provides the convenience of viewing your account from anywhere you have internet access. Contrary to popular belief, the use of online banking is safe. Most financial institutions use high-tech encryption systems to safeguard all of your personal information. It is up to the individual customer to take the necessary internet safety precautions.

Online Bill Pay is another safety option for any customer. Instead of placing your bill payments in the mailbox, you can easily pay them through online bill pay. All you have to do is input whatever company your bill is going to, the account number, the amount you are paying, and the date you want it sent out. The money for the bill is then taken from your account and formulated into a check to whatever company you’ve designated, all while not disclosing your account number. This way no one has access to your account number, unlike traditional checks. Not only does it keep you safe, but it also saves you time and money. You can conveniently pay your bills from all over the world and not have to pay for postage.

***Online Safety and Security Tips:***

- Never share your password, PIN, or username with anyone.
- Do not access your financial services information at Internet cafes, or other public spaces.

- Do not respond to emails appearing to be from your bank, government office or other entity that request personal information such as User IDs, passwords, PINs, Social Security Number, etc.
- Always delete email messages that appear to be spam or contain suspicious attachments.
- Do not open attachments from unknown sources.
- Update your virus protection software regularly.
- Use a firewall, especially if you have a high-speed, or "always on," connection to the Internet, such as a DSL or cable modem.
- Perform frequent scans on your computer to help detect viruses.
- Always download the latest security patches for your computer.
- Avoid using an automatic login feature that saves your password.
- Always log off of Online Services when you're finished. Do not just close or shut-down your browser.
- When selecting a password and 'secret questions and answers', don't use information easily linked to you such as your date of birth, pet's name or especially your Social Security Number.
- Use strong passwords that contain both numbers and letters.
- Avoid using passwords that are common names or phrases.
- Do not download files from strangers or unknown sites or click on email links from unknown senders.
- Set up your wireless equipment correctly. Read the instructions and follow the manufacturers recommended security implementation.

***Personal Information Safe House Keeping Tips:***

- Review your statements monthly for accuracy.
- Ask to combine statements or to receive your statement online.
- Always shred financial statements and receipts once reviewed.
- Store new and cancelled checks securely.
- Watch the expiration dates on your credit card or debit card. If your new card does not arrive, contact your bank or credit card company immediately.
- Never store your pin numbers in your wallet.

### ***Adding a Beneficiary:***

Adding a beneficiary to your account is always a good idea. With a beneficiary, you can designate what percentage of each individual account the designee receives upon your passing. This is not a substitute for a will, but may keep your loved ones from having to go to probate court to receive any funds. Unlike Power of Attorney, the beneficiary does not have access to your account or account information.

### ***Power of Attorney:***

Power of Attorney (POA) is a written authorization giving legal authority to act for another person. Power of Attorney can be a very useful tool in the event you become unable to conduct your own personal business. If you find it difficult to go to the bank to deposit or cash checks or to take care of other business because of physical illness, disability or lack of adequate, convenient transportation, you may appoint a trusted person to act for you by using a POA.

The POA is not usually given to an attorney but is more often given to a friend or relative. Great care should be exercised in choosing an agent because the POA can be abused by a negligent agent or by an unscrupulous agent. In such cases, you may lose money, and your only remedy might be a costly and difficult cause of action against the agent in court. That is a situation you certainly want to avoid.

You can revoke the POA at any time. The revocation should be in writing and communicated to the agent and to all persons or institutions that have been doing business with the agent. A POA also terminates upon the incapacity or death of the principal.

It should be noted that POA is one of the leading causes of elder abuse. Seniors should be cautious when choosing whom they designate to hold POA. The person who holds POA has access to your estate, land, bank accounts, stocks, and retirement funds. Some POA holders abuse this power by withdrawing funds for their own use. The advice and assistance of an attorney is recommended when preparing or executing any POA.

### ***Health Care Power of Attorney:***

A durable power of attorney for health care decision making gives an agent the power to make health care decisions on your behalf in case you become unable to make them for yourself. Such powers may be very broad; covering all medical decisions, or may be limited to specific medical matters.

- You should appoint a person (agent) you trust who knows how you feel about health care.
- You should also name an alternate in case your agent is unavailable or unable to serve.
- You should talk to the persons you choose in order to be sure they are willing to serve and to ensure they know how you feel about health care.

At least two persons must sign the document as witnesses when you sign it. You do not have to record your health care power of attorney to be valid. The health care power of attorney has been amended and includes a new HIPPA Authorization, clarifies designation of choices in connection with tube feeding and a notary signature is optional. The new document is effective for all documents executed on or after January 1, 2007.

### ***The Five Wishes:***

The Five Wishes met legal requirements in SC under a new law which became effective in June 2005. The Five Wishes document helps you express how you want to be treated if you are seriously ill and unable to speak for yourself. It is unique because it looks to all of a person's needs: medical, personal, emotional and spiritual.

Five Wishes also encourages discussing your wishes with your family and physician. Five Wishes lets your family and doctors know:

1. Which person you want to make health care decisions for you when you can't make them.
2. The kind of medical treatment you want or don't want.
3. How comfortable you want to be.
4. How you want people to treat you.
5. What you want your loved ones to know.

## MEDICARE

*For more information from the Lt. Governor's Office on Aging about Medicare visit our website [www.aging.sc.gov](http://www.aging.sc.gov) and look at the "Be Smart" Medicare Guide*

### ***Medicare Parts:***

- Medicare Part A: Is designed to cover inpatient hospital care as well as hospice, home health, and nursing facility care.
- Medicare Part B: Is designed to cover doctor visits and other outpatient care as well as preventive care.
- Medicare Part C: Is a combination of Part A, B, and sometimes D. It is also referred to as the Medicare Advantage Plans.
- Medicare Part D: Is designed to help lower the cost of prescription drugs and is commonly referred to as Medicare Prescription Drug Coverage.

### ***MEDICARE ADVANTAGE PLANS:***

**Medicare Advantage Plans** are healthcare plans approved by Medicare and provided by private insurance companies. There are several different types of plans:

- **Health Maintenance Organization (HMO):**  
Plans must cover all Part A and Part B health care. Most require you to go to doctors, specialists, or hospitals on the plan's list, except in an emergency.
- **Preferred Provider Organization (PPO):**  
Plans are available in a local or regional area and you may pay less if you use doctors, hospitals, and providers in their network, but pay additional costs for outside network visits.
- **Medical Savings Account (MSA):**  
Plans combine a high deductible health plan with a Medical Savings Account that beneficiaries can use to manage their healthcare costs.
- **Private Fee-for-Service (PFFS):**  
Plans allow you to go to any doctor or hospital that accepts the plan's payment. The plan decides how much it will pay and how much you will pay for the services you receive.

- **Medicare Special Needs (SNP):**

Plans are specially designed to meet the needs of people who live in certain institutions, are eligible for both Medicare and Medicaid, and/or have one or more chronic conditions.

**Medicare Advantage Plans** provide all of your Part A (Hospital Insurance) and all of your Part B (Medical Insurance) coverage and other medically necessary services just like you have under Original Medicare.

**Medicare Advantage Plans** may provide good coverage for some beneficiaries. You must make sure you can afford to pay any co-payments as well as the monthly premium. You also need to check to see if your healthcare providers are part of the plan's network or if they will accept payment.

**It is important for people who now have Original Medicare and are considering enrolling in any Medicare Advantage Plans to understand:**

- The Plan will provide your primary health coverage instead of Original Medicare.
- Original Medicare will no longer pay for your health care once you enroll in the plan.

You will be given a new Plan card, and it will replace your Medicare card.

- You will continue to pay your Part B premium even if you enroll in a Medicare Advantage Plan.
- The plan is not a Medicare Supplement Plan, and it does not replace Medicare Supplement.
- Insurance (Medigap).
- You may be charged extra co-payments or cost-sharing expenses for Medicare services.

***MARKETING AND SELLING OF MEDICARE ADVANTAGE PLANS:***

You have a lot of choices when it comes to your Medicare. Medicare Advantage Plans are health plan options approved by Medicare and run by private companies. These plans can be an alternative to traditional Medicare. Recognize the “Red Flags” before you enroll in a new plan.

- ***A sales person appears at your door uninvited.***

Strict marketing guidelines do not allow home visits unless you have given the company permission before the visit.

- ***A sales person contacts you in person or by phone and says they are with Medicare or Social Security. They may even hand you a red, white, and blue business card.***

Medicare and Social Security do not make home visits or unsolicited phone calls.

- ***A sales person tells you the plan is a Medicare Supplement Plan, and it will not affect your Original Medicare.***

The plan IS NOT a Medicare Supplement Plan. The plan will provide your primary health care coverage instead of Medicare.

- ***A sales person tells you that your doctor accepts the new plan.***

Your doctor may or may not accept the plan. It is important to contact your doctor directly and check to see if he or she will accept the new plan before you sign anything.

- ***A sales person wants to see your Medicare card and have you sign something.***

Do not show the sales person your Medicare card! Do not sign anything you have not read. Do not sign anything you do not understand.

- ***A sales person wants you to make a decision today – without taking the time to make sure you understand the new plan.***

**For more information or for help, please contact the SC I-CARE Program at:**

Insurance Counseling Assistance  
& Referral for Elders (I-CARE)  
Senior Medicare Patrol Project  
SC Access ([www.aging.sc.gov](http://www.aging.sc.gov))  
Lieutenant Governor's  
Office on Aging  
1301 Gervais Street, Suite 200  
Columbia, South Carolina 29201  
1-800-868-9095

**OR**

If you have any information about  
Medicaid provider fraud or patient  
abuse, please report it to Attorney  
General McMaster's Medicaid  
Fraud Unit at: 1-803-734-3660  
or call toll-free at: 1-888-NO  
CHEAT (1-866-662-4238)  
Tips can be made anonymously.

### ***Medicare Fraud:***

Medicare fraud is purposely billing Medicare for services that were never provided or received. Listed below are examples and Medicare fraud prevention tips provided by the Department of Health and Human Services.

Some examples of Medicare fraud include:

- Billing Medicare or another insurer for services or items you never got.
- Billing Medicare for services or equipment that is different from what you have received.
- Use of another person's Medicare card to get medical care, supplies, or equipment.
- Billing Medicare for home medical equipment after it has been returned.

### ***Detection Tips:***

You should be suspicious if the provider tells you that:

- The test is free; he only needs your Medicare number for his records.  
NOTE: For clinical laboratory tests, there is no co-payment and a provider may in good faith state that the test is free, since there is no cost to the person with Medicare.
- Medicare wants you to have the item or service.
- They know how to get Medicare to pay for it.
- The more tests they provide the cheaper they are.
- The equipment or service is free; it won't cost you anything.

Be suspicious of providers that:

- Charge co-payments on clinical laboratory tests, and on Medicare covered preventive services such as PAP smears, prostate specific antigen (PSA) tests, or flu and pneumonia shots.
- Routinely waive co-payments on any services, other than those previously mentioned, without checking your ability to pay.
- Advertise "free" consultations to people with Medicare.
- Claim they represent Medicare.



- Use pressure or scare tactics to sell you high priced medical services or diagnostic tests.
- Bill Medicare for services you did not receive.
- Use telemarketing and door-to-door selling as marketing tools.

***Prevention Tips:***

To help prevent Medicare fraud, you should report suspected instances of fraud. Whenever you receive a payment notice from Medicare, review it for errors. The payment notice shows what Medicare was billed for, what Medicare paid and what you owe. Make sure Medicare was not billed for health care services or medical supplies and equipment you did not receive.

The following is a list of tips to prevent fraud:

- **Don't** ever give out your Medicare Health Insurance Claim Number (on your Medicare card) except to your physician or other Medicare provider.
- **Don't** allow anyone, except appropriate medical professionals, to review your medical records or recommend services.
- **Don't** contact your physician to request a service that you do not need.
- **Do** be careful in accepting Medicare services that are represented as being free.
- **Do** be cautious when you are offered free testing or screening in exchange for your Medicare card number.
- **Do** be cautious of any provider who maintains they have been endorsed by the federal government or by Medicare.
- **Do** avoid a provider of health care items or services who tells you that the item or service is not usually covered, but they know how to bill Medicare to get it paid.

It is in your best interest and that of all citizens to report suspected fraud. Health care fraud, whether against Medicare or private insurers, increases everyone's

health care costs, much the same as shoplifting increases the costs of the food we eat and the clothes we wear. If we are to maintain and sustain our current health care system, we must work together to reduce costs.

## **How You Can Help Yourself**

---

### ***Credit Card Purchases:***

If your claim involves a dispute of charges placed on your credit card or billing statement or if a merchant has promised to reverse or credit your charge card but has failed to do so, you must act quickly to preserve your right to challenge a charge.

Under the Federal Fair Credit Billing Act, your credit card company must receive a written dispute notice from you within 60 days after the first bill containing the disputed charge was mailed to you. We cannot dispute this charge for you. Look at the back of your credit card statement for specific information regarding the procedure for filing your dispute. You must file your dispute with your credit card company; a complaint to the merchant or company that made the charge is not sufficient. Even if you file a credit card dispute, you can still file a claim with our office.

It is preferable that you try to resolve your own complaint before contacting the Bureau of Consumer Protection. Instruction to do so follows. However, if you have exhausted your efforts to resolve the problem without success, contact the Office of the Attorney General immediately for assistance.

### ***Identify the Problem:***

Before you complain to a company, be sure to identify the problem, what (if anything) you have already done to resolve the problem and decide what you think is a fair settlement. For example, do you want your money back? Would you like the product repaired? Do you want the product exchanged?

### ***Gather Records:***

Start a file about your complaint. Include copies of sales receipts, repair orders, warranties, canceled checks, and contracts which will back up your complaint and help the company solve your problem.

Go back to where you made the purchase. Contact the person who sold you the item or performed the service. Calmly and accurately explain the problem and what action you would like to have taken. If that person is not helpful, ask for the supervisor or manager and restate your case. A large percentage of consumer problems are resolved at this level. Chances are yours will be too.

Allow each person you contact time to resolve your problem before contacting another source of assistance. Keep a record of your efforts and include notes about who you spoke with and what was done about the problem. Save copies of any letters you send to the company as well as letters sent to you.

### ***Writing a Complaint Letter:***

The letter should include your name, address, home and work telephone numbers, and account number, if appropriate. Make your letter brief and to the point.

Specify all the important facts about your purchase, including the date and place you made the purchase and any information you can give about the product, such as the serial or model number. If you are writing to complain about a service you received, describe the service and who performed it.

State exactly what you want done about the problem and how long you are willing to wait to resolve it. Be reasonable. Include copies of all documents regarding your problem. Be sure to send COPIES, not originals.

Don't write an angry, sarcastic, or threatening letter. The person reading your letter probably was not responsible for your problem, but may be very helpful in resolving it. Type your letter if possible. If it is handwritten, make sure it is neat and easy to read. Keep a copy of all correspondence to and from the company as well as a copy of your complaint.

### **Filing a Complaint with the SC Department of Consumer Affairs**

The following information is being provided to assist you in filing a complaint with the Department of Consumer Affairs. Help us help you by providing the additional documents requested, such as a copy of your contract, warranty, canceled checks, receipts, bill of sale or Buyer's Guide as appropriate.

Your complaint will be given a number and assigned to a complaint analyst who will evaluate it to determine if the Department can assist you. Note: If your complaint falls within the jurisdiction of another agency, South Carolina law requires that we forward your complaint to that agency and you will be notified. If you are represented by an attorney or if legal action has been taken, the Department cannot intercede or interfere in that process. The Department does not have jurisdiction in business to business complaints or complaints between two individuals.

Once an analyst determines that you have a complaint that can be handled by the Department, the business you are complaining against will be contacted in writing for a response or suggested resolution. Due to limited staff and budgetary constraints, we are unable to handle complaints by telephoning the business.

Several letters will be sent to the business in an effort to obtain a reply. We will send a card to you in approximately 30 days if we have not heard from the business. Often the business will contact you immediately with an offer of a goodwill resolution to the complaint. Please contact the Department if your complaint is resolved before you hear from us.

After a reply is received from the business, the analyst will compare the facts presented in your complaint and the facts given by the business. We encourage your participation in negotiating an amicable solution.

We will contact you if we do not receive a response from the business. If the business does not respond to our letters, the analyst will evaluate the complaint to determine if additional efforts are needed, such as Department enforcement, referral to another source or close the file.

The Department cannot always resolve complaints to the satisfaction of the consumer; however, we will try to determine the obligation of the business based on the facts and advise you. Our complaint analysts are knowledgeable about consumer rights and have access to attorneys who provide legal guidance to them. The Department resolves a large number of complaints which require varying lengths of time to resolve. Your patience is appreciated and we will contact you as soon as possible.

### **Filing a Complaint with the Lieutenant Governor's Office on Aging**

To file a complaint with the Lieutenant Governor's Office on Aging, please fill out the attached complaint form and return it to the address below. Or, you can submit it electronically by accessing it online at [www.sc.aging.gov](http://www.sc.aging.gov). Once we receive your complaint, we will work diligently in hopes of resolving your problem. Please contact 1-803-734-9900 with any further questions or concerns you may have regarding your complaint.

#### **The Lieutenant Governor's Office on Aging**

1301 Gervais Street, Suite 200

Columbia, SC 29201

Phone: (803) 734-9900

**South Carolina  
Lieutenant Governor  
Office on Aging**



**Fraud Complaint Form**

**André Bauer  
Lieutenant Governor**

**The Lieutenant Governor's  
Office on Aging**

Date: \_\_\_\_\_

Location: \_\_\_\_\_

1301 Gervais Street, Suite 200  
Columbia, SC 29201  
Phone: (803) 734-9900  
E-mail: [scams@aging.sc.gov](mailto:scams@aging.sc.gov)  
Web address: [www.aging.sc.gov](http://www.aging.sc.gov)

**Your Name**

**Address**

**City**

**State**

**Zip**

**County**

**Home Phone Number**

**Cell**

**E-mail Address**

**Name of Suspect Individual or Organization**

**Name of Individual to Whom You Complained**

**Address**

**City**

**State**

**Zip**

**County**



## Resources

---

For more information on frauds and schemes, please log on to the following web sites. They are filled with information on current and past schemes, as well as ways to prevent being victimized by scammers.

South Carolina Department of Consumer Affairs <http://www.scconsumer.gov/>

Federal Trade Commission - [www.ftc.gov](http://www.ftc.gov)

Federal Bureau of Investigation - [www.fbi.gov/majcases/fraud/fraudschemes.htm](http://www.fbi.gov/majcases/fraud/fraudschemes.htm)

National Consumer League - <http://www.nclnet.org>

Wachovia Bank - [www.wahociva.com](http://www.wahociva.com)

Medicare - [www.medicare.gov](http://www.medicare.gov)

South Carolina Bar Association - [www.scbar.org](http://www.scbar.org)

South Carolina Attorney General's Office - <http://www.scattorneygeneral.org/>

AARP - <http://www.aarp.org/states/sc/>

Better Business Bureau - [www.columbia.bbb.org](http://www.columbia.bbb.org)

Wells Fargo Bank - [www.wellsfargo.com/](http://www.wellsfargo.com/)

BITS - <http://www.bitsinfo.org/downloads/Publications%20Page/bitstoolfeb06.pdf>

Illinois State Attorney's Office - [http://www.willcountysao.com/identity\\_theft-protecting\\_yourself.htm](http://www.willcountysao.com/identity_theft-protecting_yourself.htm)

Colorado District Attorney's Office - [www.co.larimer.co.us/da/elder\\_fraud.pdf](http://www.co.larimer.co.us/da/elder_fraud.pdf)